REMARKS

The Office Action dated May 7, 2004, has been received and carefully noted. The above amendments to the claims, and the following remarks, are submitted as a full and complete response thereto.

Claims 1-32, 34-38, 41-45, 47-53, 55-56 and 59 have been amended to more particularly point out and distinctly claim the subject matter of the invention. Claims 57 and 58 are canceled without prejudice or disclaimer of the subject matter thereof. No new matter has been added. Claims 1-56 and 59 are pending in the present application and are respectfully submitted for consideration.

Claims 1-23 and 25-58 were rejected under 35 U.S.C. §102(b) as allegedly being anticipated by U.S. Patent No. 5,548,649 (*Jacobson*). The Office Action took the position that *Jacobson* taught all the features of these claims including independent claims 1, 25, 26, 27, 37, 41, 42, 55 and 56. Applicant respectfully submits that *Jacobson* does not disclose or suggest all the features of the presently pending claims.

Claim 1, upon which claims 2-24 are dependent, recites a method for secure communication between a first end terminal located in a first secure network and a second end terminal located in a second secure network. The first and second networks are separated by a relatively insecure intermediate network. The method includes selectively routing a predetermined type of communication identified by a trigger from the first end terminal to the second end terminal over the relatively insecure intermediate network by means of at least one network element triggerable to refer to information held

in a storage means to selectively route the communication according to the information held in the storage means. The method also includes encrypting the selectively routed communication by means of an encryption engine before it traverses the intermediate network. The at least one network element and the encryption engine are located substantially within the first secure network.

Claim 25 recites a method for the distribution of security information between a first node and at least one second node, including the step of providing at least one network element operable to store security information and triggerable to distribute the security information from the first node to at least one target node.

Claim 26 recites a method for the distribution of security information between a first node in a first secure network and at least one node in a second secure network. The first and the second networks are separated by a relatively insecure network. Communications from the first node to the at least one second node via the relatively insecure network are encrypted, including the step of providing at least one network element operable to store security information and triggerable to distribute the security information in a secure manner from the first node to at least one target node in the second secure network.

Independent claim 27 recites a secure network arrangement having some of the features discussed in claim 1 above. Independent claim 37 recites a secure network arrangement having some of the features discussed in claim 1 above. Claim 41 recites a method for the distribution of security information having some of the features of claim

26 discussed above. Claims 42 and 56 recite a network arrangement having some of the features of claim 26, discussed above. Claim 55 recites a network arrangement having some of the features of claim 25, discussed above.

As discussed in the specification, examples of the present invention enables subscribers to benefit from a secure network service customized according to their own preferences. Further, specific encryption algorithms may be used between certain end terminals. Thus, secure communication between end terminals may be achieved that are in first and second secure networks. It is respectfully submitted that *Jacobson* fails to disclose or suggest all the elements of any of the presently pending claims. Therefore, *Jacobson* fails to provide the critical and unobvious advantages discussed above.

Jacobson relates to a network local security bridge for bridging first and second sides of a network. Referring to Figure 1 of *Jacobson*, Ethernet network 100 is shown along with various devices such as host 102-1 to 102-10, network security bridges 104-1 to 104-3, and gateway 106. *Jacobson* describes a first side that includes a local secure zone and a second side that includes a remote secure zone. The local security bridge of bridges 104-1 to 104-3 receives first and second side packets from the first and second sides of the network, respectively. First side packets are encrypted by the local security bridge if their destination address is within the remote secure zone, but are not encrypted if their destination address is within a remote insecure zone. Second side packets are decrypted if they originate from the remote secure zone, but not if they originate from an insecure zone. After any necessary encryption or decryption, first and second side

packets are transmitted to their destination by the local security bridge. *Jacobson*, however, does not disclose or suggest selectively routing a predetermined type of communication identified by a trigger from the first end terminal to the second end terminal over a relatively insecure intermediate network by means of at least one network element triggerable to refer to information held in a storage means to selectively route the communication according to the information held in the storage means.

In contrast, claim 1 recites "selectively routing a predetermined type of communication identified by a trigger from the first end terminal to the second end terminal over said relatively insecure intermediate network by means of at least one network element triggerable to refer to information held in a storage means to selectively route said communication according to said information held in said storage means." In addition, claim 25 recites "providing at least one network element operable to store security information and triggerable to distribute the security information from said first node to at least one target node." The remaining independent claims recite subject matter similar to claims 1 and 25. Applicant submits that *Jacobson* does not disclose or suggest at least these features of the independent claims.

Claim 1 is not anticipated by *Jacobson* because *Jacobson* does not disclose or suggest first and second secure networks that are separated by a relatively insecure network. *Jacobson* merely describes security issues within a single network. Further, *Jacobson* does not disclose or suggest selectively routing a predetermined type of communication. Because of selectively routing, according to examples of the present

invention, the encryption service may or may not be selected for use depending on the type of communication. *Jacobson* also does not disclose or suggest network elements triggerable to refer to information held in a storage means to selectively route the communication according to the information stored in the storage means. The information stored in the storage means may relate to the security required for specific communications between particular end terminals, including whether or not the insecure network is to be used for transmitting packets. Instead, *Jacobson* describes encrypting packets by the local security bridge if a destination address is within a remote secure zone. *Jacobson* does not disclose or suggest selecting a route for the encrypted packets. Thus, *Jacobson* does not disclose or suggest selectively routing a predetermined type of communication by means of at least one network element triggerable to refer to information held in the storage means.

Claim 25 recites distributing security information from a first node to at least one target node. *Jacobson* also fails to disclose or suggest this feature and merely describes transmitting encrypted and decrypted packets from one node to another within a network. *Jacobson* does not disclose or suggest distributing the secured information that is used for encrypting and decrypting the packets. According to examples of the present invention, private keys may be distributed to specific subscribers so that the subscribers exclusively receive certain data. This feature may be possible by distributing security information to certain target nodes. *Jacobson* does not disclose or suggest distributing security information to certain target nodes that provide at least one network element operable to

store security information and triggerable to distribute the security information from the first node to at least one target node. Thus, *Jacobson* does not disclose or suggest at least these features of the pending claims.

As noted above, the remaining independent claims recite subject matter similar to claim 1 and/or claim 25 and are allowable for at least these reasons. Thus, for at least the reasons given above, the remaining independent claims 26, 27, 37, 41, 42, 55 and 56 are not disclosed or suggested by *Jacobson*.

Claims 2-23 and 28-36 and 38-40 and 43-54 are directly or indirectly dependent upon the independent claims discussed above. The dependent claims are allowable at least for the reasons given above, and because they recite subject matter in addition to the subject matter of the independent claims. Thus, it is submitted that claims 1-23 and 25-56 are not anticipated by *Jacobson*. Applicant respectfully requests that the anticipation rejection be withdrawn.

Claims 24 and 59 were rejected under 35 U.S.C. §103(a) as allegedly being unpatentable over *Jacobson* in view of U.S. Patent No. 6,421,339 (*Thomas*). The Office Action took the position that *Jacobson* does not teach providing to a subscriber in a visited network by virtue of a roaming agreement between the operator of the visited network and the operator of the subscriber's home network. The Office Action then took the position that *Thomas* taught this feature and that it would have been obvious to a person having ordinary skill in the art at the time the invention was made to include such roaming agreement in *Jacobson*'s network security bridging system to have a capability

to call a H.323 compliant data packet network. Applicant submits that the cited references, either alone or in combination, do not disclose or suggest all the features of the presently pending claims.

Claim 24 depends directly from claim 1, and claim 59 depends indirectly from claim 1. Claim 1 is summarized above. Further, *Jacobson* does not disclose or suggest all the features of claim 1. Applicant submits that *Thomas* does not disclose or suggest those features of claim 1 missing from *Jacobson.*

Thomas relates to methods and systems for call-forwarding. *Thomas* describes a compliant data packet network with a registering function whereby home-based users are identified separate from visiting users having other networks as home bases. The user location data of *Thomas* may be retrieved and/or modified as those users roam to other compliant networks and register with a gatekeeper at that visited network. The registration of a visiting user with a visited gatekeeper includes the process of assigning a transient identity to the roaming user, obtaining confirmation from the home gatekeeper that roaming is authorized when registering the roaming user's present address and transient identity at the home site so that calls received at the home network can be directed to the user at the visited site. *Thomas*, however, when combined with *Jacobson*, does not disclose or suggest selectively routing a predetermined type of communication identified by a trigger from the first end terminal to a second end terminal over a relatively insecure intermediate network by means of at least one network element

triggerable to refer information held in a storage means to selectively route the communication according to the information held in the storage means.

As noted above, claim 1 recites "selectively routing a predetermined type of communication identified by a trigger from the first end terminal to the second end terminal over said relatively insecure intermediate network by means of at least one network element triggerable to refer to information held in a storage means to selectively route said communication according to said information held in said storage means." Applicant submits that *Thomas* does not disclose or suggest at least this feature of claim 1.

As stated by the Office Action, *Thomas* is cited as teaching the providing to a subscriber in a visited network by virtue of a roaming agreement between the operator of the visited network and the operator of the subscriber's home network. This aspect of *Thomas* does not disclose or suggest selectively routing a predetermined type of communication over a relatively insecure intermediate network by means of one or more network elements according to information in a storage means. Therefore, applicant submits that *Thomas* does not disclose or suggest those features missing from *Jacobson.*

Further, claims 24 and 59 are directly or indirectly dependent upon independent claim 1. Because independent claim 1 is non-obvious over the cited references, claims 24 and 59 also are non-obvious. If an independent claim is non-obvious, then any claim depending therefrom also is non-obvious. MPEP 2143.03. Thus, claims 24 and 59 are

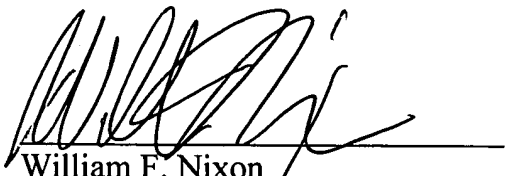
not rendered obvious by the cited references and applicant respectfully requests that the obviousness rejection be withdrawn.

It is submitted that each of claims 1-56 and 59 recite subject matter that is neither disclosed nor suggested by the cited references. It is therefore respectfully requested that all the claims be allowed, and this application passed to issue.

If for any reason the Examiner determines that the application is not now in condition for allowance, it is respectfully requested that the Examiner contact, by telephone, the applicant's undersigned attorney at the indicated telephone number to arrange for an interview to expedite the disposition of this application.

In the event this paper is not being timely filed, the applicant respectfully petitions or an appropriate extension of time. Any fees for such an extension together with any additional fees may be charged to Counsel's Deposit Account 50-2222.

Respectfully submitted,



William F. Nixon
Registration No. 44,262

Customer No. 32294
SQUIRE, SANDERS & DEMPSEY LLP
14TH Floor
8000 Towers Crescent Drive
Tysons Corner, Virginia 22182-2700
Telephone: 703-720-7800
Fax: 703-720-7802

WFN:cct